(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 081 884 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
07.03.2001 Patentblatt 2001/10

(51) Int. Cl.[7]: **H04H 1/00**, H04N 7/16

(21) Anmeldenummer: **00118546.1**

(22) Anmeldetag: **25.08.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **03.09.1999 DE 19941929**

(71) Anmelder: **ROBERT BOSCH GMBH**
70442 Stuttgart (DE)

(72) Erfinder: **Schneiders, Peter**
41141 Hildesheim (DE)

(54) Verfahren zur Übertragung von verschlüsselten Daten über ein Rundfunknetz, wobei die Entschlüsselungsdaten über eine Duplex-Fernmeldeverbindung angefordert werden

(57) Es wird ein Verfahren zur Übertragung von verschlüsselten Daten vorgeschlagen, das dazu dient, einerseits verschlüsselte Daten nur bestimmten Nutzern zugänglich zu machen und andererseits einen Datensatz von bestimmten Nutzern zu aktualisieren. Das Verfahren zur Übertragung von verschlüsselten Daten umfaßt die Versendung der Entschlüsselungsdaten mittels eines Duplex-Übertragungsverfahrens und die Versendung der verschlüsselten Daten mittels eines Rundfunkübertragungsverfahrens. In einer Weiterbildung umfaßt das Verfahren die Versendung von Datensätzen mittels des Duplex-Übertragungsverfahrens zu einem jeweiligen Nutzer und die Übertragung von Zusatzdaten, um die Datensätze zu aktualisieren mittels des Rundfunkübertragungsverfahrens. Bei beiden Ausführungen fordert der Nutzer entweder die Entschlüsselungsdaten oder den Datensatz durch Anwahl eines Datendienstanbieters an. Sowohl die Entschlüsselungsdaten als auch der ursprüngliche Datensatz sind nur für eine vorgegebene Zeit für einen Nutzer nutzbar. Dem Nutzer wird die Übertragungszeit über das Duplex-Übertragungssystem in Rechnung gestellt, so daß damit die Bereitstellung der Datendienste bezahlt wird.

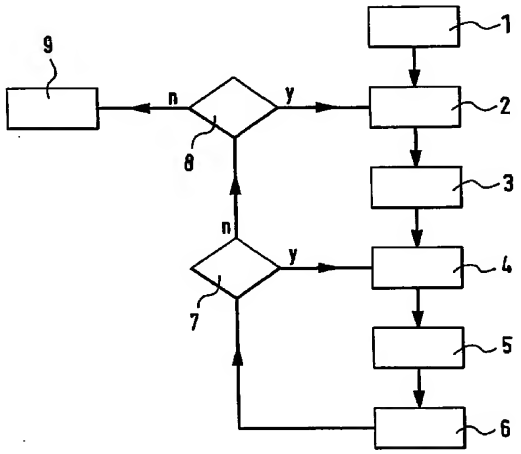

Fig. 1

EP 1 081 884 A2

Beschreibung

Stand der Technik

[0001] Die Erfindung geht aus von einem Verfahren zur Übertragung von verschlüsselten Daten bzw. nach der Gattung des unabhängigen Patentanspruchs.

[0002] Es ist bereits aus der Broschüre „Digital Audio Broadcasting", Eureka - 147 Project, April 1996 bekannt, daß bei DAB (Digital Audio Broadcasting) Programme und/oder Daten für einen bestimmten Empfängerkreis ausgestrahlt werden können. Diese Betriebsart wird mit dem englisch sprachigen Begriff conditional access bezeichnet, also einem privilegierten Zugang zu diesen Programmen und/oder Daten. Dafür sind diese Programme und/oder Daten verschlüsselt, wobei die berechtigten Empfänger entweder einen Schlüssel mitübertragen bekommen, um die Programme zu entschlüsseln, oder eine Speichermöglichkeit an ihrem Empfänger aufweisen, wie z.B. eine Smartcard, die zumindest die Daten enthält, um einen Schlüssel zu entschlüsseln oder um sogar das ganze Programm und/oder die Daten zu entschlüsseln. Eine Smartcard weist einen Mikroprozessor auf, der Informationen speichert, verarbeitet und verwaltet. Mittels einer Geheimnummer und/oder Verschlüsselungstechniken sind einer Smartcard ein hohes Maß an Sicherheit hinzugefügt.

[0003] Ist die Zugangsberechtigung mittels der Smartcard zeitbegrenzt, wird sich der Kunde nach Ablauf der Gültigkeit seiner Smartcard eine weiterhin gültige Smartcard beschaffen oder die Gültigkeit seiner Smartcard verlängern lassen.

Vorteile der Erfindung

[0004] Das erfindungsgemäße Verfahren mit den Merkmalen des unabhängigen Patentanspruchs hat demgegenüber den Vorteil, daß der Schlüssel zur Entschlüsselung der verschlüsselten Programme und/oder Daten, die mittels eines Rundfunkübertragungaverfahrens wie DAB übertragen werden, mittels eines Duplex-Übertragungsverfahrens, wie z.B. ein Mobilfunkübertragungsverfahren, übertragen wird, so daß der Nutzer die empfangenen Daten entschlüsseln kann. Dadurch ist der Nutzer in der Lage, sich jederzeit und von jedem Ort den notwendigen Schlüssel zur Entschlüsselung der verschlüsselten Daten zu beschaffen. Er gewinnt damit ein großes Maß an Flexibilität. Darüber hinaus braucht der Benutzer, den notwendigen Schlüssel sich nur zu beschaffen, wenn er die verschlüsselten Programme und/oder Daten tatsächlich empfangen möchte.

[0005] Darüber hinaus ist es von Vorteil, daß die Erfindung auf bereits vorhandene Infrastruktur zurückgreift, denn sowohl ein Rundfunkverteilsystem als auch verschiedene Mobilfunksysteme sind bereits installiert und können genutzt werden.

[0006] Als weiterer Vorteil ist anzusehen, daß mittels des Duplex-Übertragungsverfahrens ein Datensatz zu einem Nutzer übertragen wird und daß mittels des Rundfunkübertragungssystems dann laufend aktualisierte Zusatzdaten übertragen werden, die mit diesem Datensatz genutzt werden. Dadurch ist es möglich, daß ein Nutzer nur einmal über ein Duplex-Übertragungsverfahren einen Datensatz empfängt und ihn dann mittels der Zusatzdaten, die über ein Rundfunkübertragungssystem übertragen werden, aktualisiert. Diese Methode der Aktualisierung ist sowohl für den Datendienstanbieter als auch für den Kunden äußerst kostengünstig.

[0007] Durch die in den abhängigen Ansprüchen aufgeführten Maßnahmen sind vorteilhafte Weiterbildungen und Verbesserungen der in den unabhängigen Ansprüchen angegebenen Verfahren möglich.

[0008] Besonders vorteilhaft ist, daß der Nutzer, wenn er die verschlüsselten Daten entschlüsseln will oder wenn er einen Datensatz laden möchte, mittels des Duplex-Übertragungsverfahrens den Datenanbieter anwählt und sich entweder den Schlüssel oder den Datensatz von dem Datendienstanbieter lädt. Dadurch ist der Nutzer völlig frei zu bestimmen, wann, wo und was er für Datendienste nutzen möchte. Es ist dabei zu beachten, daß solche Datendienste und verschlüsselten Daten von verschiedenen Datendienstanbietern angeboten werden, so daß der Nutzer auf einer Opportunitätsbasis den von ihm jeweils gewünschten Datendienstanbieter anwählt.

[0009] Weiterhin ist es von Vorteil, daß sowohl der Schlüssel als auch der Datensatz, den sich der Nutzer jeweils mittels des Duplex-Übertragungsverfahrens lädt, eine zeitbegrenzte Gültigkeit hat. Dadurch ist es für den Datendienstanbieter möglich, seinen Datendienst für eine bestimmte Zeit anzubieten und zu berechnen. Außerdem ist es dem Nutzer transparent, wie lange der von ihm gewünschte Datendienst ihm zur Verfügung steht.

[0010] Darüber hinaus ist es von Vorteil, daß der Datendienstanbieter dem Nutzer die Übertragungszeit für die Entschlüsselungsdaten und/oder den Datensatz berechnet, so daß der Nutzer einen für die Gültigkeitsdauer entsprechenden Betrag für die Übertragungszeit dieser notwendigen Daten, um den Datendienst zu nutzen, bezahlt. Dies ist dann ein sehr einfaches Abrechnungssystem für einen Datendienstanbieter, da er durch den Betrag, den er für die Übertragungszeit des Schlüssels oder des Datensatzes verlangt, gleichzeitig seinen Datendienst vermietet. Darüber hinaus ist dieses Abrechnungssystem auch für den Nutzer von großer Transparenz, da er zum Beispiel über seine Telefonrechnung, wenn er ein Mobilfunknetz benutzt, die Kosten für den Datendienst entnehmen kann.

Zeichnung

[0011] Ausführungsbeispiele der Erfindung sind in der Zeichnung dargestellt und in der nachfolgenden

Beschreibung näher erläutert. Es zeigen Figur 1 ein Verfahren zur Übertragung von verschlüsselten Daten und Figur 2 ein Verfahren zur Übertragung von Datensätzen.

Beschreibung der Ausführungsbeispiele

[0012] Durch die Einführung von digitalen Rundfunkübertragungsverfahren wie z.B. DAB sind attraktive Möglichkeiten gegeben, um Datendienste über das Rundfunkverteilnetz zu übertragen.

[0013] DAB ist ein digitales Rundfunkübertragungsverfahren, das insbesondere für den mobilen Empfang geeignet ist. Durch den Einsatz des sog. orthogonalen Frequenzmultiplex wird insbesondere eine frequenzselektive Dämpfung in ihrer Wirkung auf das übertragene Signal stark reduziert. Das Signal, das mittels orthogonalem Frequenzmultiplex übertragen wird, wird bei DAB sendeseitig auf mehrere Frequenzen verteilt, wobei sich die Signalanteile auf den verschiedenen Frequenzen gegenseitig nicht beeinflussen. Dieses Verhalten wird mit orthogonal beschrieben. Dadurch wird erreicht, daß eine frequenzselektive Dämpfung nur die Signalkomponente stört, die auf der Frequenz, die einer starken Dämpfung unterliegt, übertragen wird.

[0014] Darüber hinaus wird das Signal im Sender einer Kanalcodierung unterzogen, wobei den ursprünglichen Daten zusätzliche Daten hinzugefügt werden, so daß Fehler im Empfänger unter Ausnutzung dieser zusätzlichen Daten korrigiert werden können. Weiterhin hat DAB die Eigenschaft, daß neben den Audiodaten auch weitere Daten gleichzeitig übertragen werden, wobei die Größe und die Aufteilung dieser Daten frei gestaltbar sind. DAB weist eine Rahmenstruktur auf, die Rahmenfelder aufweist, mittels derer ein Empfänger erkennt, welcher Inhalt in dem jeweiligen Rahmen übertragen wird. In einem Rahmenfeld steht zum Beispiel die Information, daß von einem bestimmten Datendienstanbieter Daten für ein Navigationssystem in diesem Rahmen enthalten sind. Sucht der Empfänger nach diesen Daten, wertet der Empfänger diesen Rahmen aus, um die Daten zu erhalten.

[0015] Aber auch andere digitale Rundfunk- und Fernsehübertragungsverfahren, wie DVB (Digital Video Broadcasting) oder DRM (Digital Radio Monial) bieten die Möglichkeit, Daten zu übertragen. Diese Übertragungsverfahren weisen auch den orthogonalen Frequenzmultiplex auf, sie unterscheiden sich von DAB insbesondere durch den Sendefrequenzbereich, die Rahmenstruktur und die Übertragungsbandbreite.

[0016] Digitale zellulare Mobilfunkübertragungsverfahren wie GSM (Global System for Mobile Communication) oder UMTS (Universal Mobile Telecommunication System) haben im Vergleich zu den Rundfunkübertragungsverfahren die Eigenschaft, daß eine Verbindung zu bestimmten Nutzern hergestellt wird und nicht ein ganzes Gebiet versorgt wird, ohne die einzelnen Nutzer in diesem Gebiet direkt anzuwählen. Die Nutzer müssen also hier direkt angewählt werden, während bei einem Rundfunkübertragungsverfahren jeder eingeschaltete Empfänger die Daten empfängt.

[0017] Wird bei der Verteilung eines Datendienstes die Kombination eines Rundfunkübertragungsverfahrens und eines Duplex-Übertragungsverfahrens, wie es Mobilfunkübertragungsverfahren sind, genutzt, so ergeben sich vorteilhafte Möglichkeiten, um einen Datendienst nur einem bestimmten Nutzerkreis verfügbar zu machen.

[0018] Duplex-Übertragungsverfahren haben die Eigenschaft, daß Daten in beiden Richtungen übertragen werden, d.h. daß miteinander kommunizierende Stationen sowohl Sender als auch Empfänger sind. Telefon- und Mobilfunkverbindungen sind Beispiele dafür.

[0019] Rundfunkübertragungsverfahren dagegen sind Simplex-Übertragungsverfahren, da nur eine Station sendet und viele andere Stationen empfangen. Bei einigen Funkübertragungssystemen wird ein sogenannter Halbduplex verwendet, d.h. wenn eine Station sendet, kann die andere Station nur empfangen, während bei einem Duplex-Übertragungsverfahren beide Stationen gleichzeitig senden können.

[0020] Wird ein Datendienst nur einem bestimmten Empfängerkreis zugänglich gemacht, so wird dies mit Verschlüsselung erreicht. Verschlüsselung wird hier in einer Weise durchgeführt, so daß die Daten mit Pseudo-Zufallszahlen kombiniert werden, wobei diese Pseudo-Zufallszahlen mit einem Pseudo-Zufallsgenerator erzeugt werden und wobei dieser Pseudo-Zufallsgenerator mit einem Initialisierungswort, das durch einen Zufallsgenerator erzeugt wird, initialisiert wird. Ein Zufallsgenerator ist zum Beispiel ein Rauschgenerator, mit dem zufällige Zahlen erzeugt werden können.

[0021] Im übrigen sind andere Verschlüsselungsarten denkbar, dazu zählt zum Beispiel die Verwürfelung von Datenstrukturen.

[0022] Alternativ kann eine große Zahl von einmal erzeugten Zufallszahlen in einem Speicher abgelegt werden, um bei Bedarf für die Initialisierung des Pseudozufallsgenerators herangezogen zu werden.

[0023] Pseudo-Zufallszahlen haben die Eigenschaft, daß, wenn man das Initialisierungswort kennt, alle folgenden Pseudo-Zufallszahlen berechnen werden können, weil die Rechenvorschrift, mit der der Pseudozufallsgenerator die Pseudozufallszahlen erzeugt, dem Empfänger bekannt ist. Um also Daten, die mit Pseudo-Zufallszahlen verschlüsselt worden sind, zu entschlüsseln, ist es notwendig, daß das Initialisierungswort im Empfänger bekannt ist. Es dient also als Schlüssel. Dann kann der Empfänger mittels eines Pseudo-Zufallsgenerators die gleichen Pseudo-Zufallszahlen erzeugen und durch eine weitere Verknüpfung dieser Pseudo-Zufallsworte mit den verschlüsselten Daten diese Daten wieder entschlüsseln.

[0024] Verknüpft man im Sender die Daten mit den Pseudo-Zufallsworten mittels einer Exclusiv-Oder-Ver-

knüpfung, dann entschlüsselt man die Daten im Empfänger durch eine weitere Exclusiv-Oder-Verknüpfung des verschlüsselten Datenwortes mit der gleichen Pseudo-Zufallszahl. Denn, wird eine Zahl x1 zweimal mit einer anderen Zahl x2 exclusiv-oder-verknüpft, ist das Ergebnis wieder die ursprüngliche Zahl x1.

[0025] In Figur 1 ist ein Verfahren zur Übertragung von verschlüsselten Daten als Flußdiagramm dargestellt. In Verfahrensschritt 1 wird das Verfahren begonnen. In Verfahrensschritt 2 wählt ein Nutzer über ein Duplex-Übertragungsverfahren einen Datendienstanbieter an, um von einem Datendienstanbieter einen Schlüssel zur Entschlüsselung der verschlüsselten Daten anzufordern.

[0026] In Verfahrensschritt 3 wird von dem Datendienstanbieter mittels des Duplex-Übertragungsverfahrens der Schlüssel zur Entschlüsselung der verschlüsselten Daten, die mit einem Rundfunkübertragungssystem versendet werden, übertragen. Dazu ist eine Sende-/Empfangsstation für ein Duplex-Übertragungsverfahren mit einem Rundfunkempfänger verbunden, so daß ein Datentransfer von der Sende-/Empfangsstation zum Rundfunkempfänger möglich ist. Der Schlüssel wird also von der Sende-/Empfangsstation empfangen und als Datum an den Rundfunempfänger übergeben, damit der Rundfunempfänger die verschlüsselten Daten entschlüsseln kann.

[0027] Den Datendienstanbieter wählt der Nutzer durch direkte Eingaben an seinem Rundfunkempfänger aus, oder der Rundfunkempfänger hat eine Liste mit verschiedenen Datendienstanbietern abgespeichert, aus denen der Nutzer einen Datendienstanbieter auswählt und der Rundfunkempfänger dann automatisch diesen Datendienstanbieter mittels der Sende-/Empfangsstation anwählt.

[0028] In Verfahrensschritt 4 empfängt der Nutzer mittels eines Rundfunkempfängers die verschlüsselten Rundfunkdaten. In Verfahrensschritt 5 entschlüsselt der Nutzer mittels seines Schlüssels die empfangenen verschlüsselten Daten im Rundfunkempfänger.

[0029] In Verfahrensschritt 6 stellt der Nutzer die entschlüsselten Daten mittels akustisch und/oder optischer Mittel zur Darstellung dar, um sie sich ansehen bzw. lesen zu können. Die Daten werden z.B. in einem Navigationssystem benutzt, um die aktuelle Verkehrslage auf einer Anzeige darzustellen, um damit den schnellstmöglichen Weg für einen Autofahrer zu seinem Ziel zu berechnen und um dem Autofahrer damit seinen optimalen Weg zu seinem Ziel anzuzeigen.

[0030] Andere Möglichkeiten sind, daß sich der Nutzer aktuelle Börsendaten auswählt oder daß sich ein Nutzer verschlüsselte Rundfunkprogramme anhört oder daß sich z.B. eine Baufirma bestimmte Daten zu einem Baugelände hin überträgt oder daß sich die Polizei mit einem solchen Verfahren wichtige Daten von Datenbanken zu ihrem Einsatzort holt. Dabei gewährt die Verschlüsselung, daß nur die berechtigten Teilnehmer mit dem Schlüssel die Daten entschlüsseln können. Ist eine hohe Sicherheit wie bei der Polizei notwendig, wird zum Beispiel zusätzlich noch eine Smartcard verwendet, um den Schlüssel zur Entschlüsselung mittels eines Duplex-Übertragungsverfahrens empfangen zu können.

[0031] In Verfahrensschritt 7 wird überprüft, ob der Schlüssel noch gültig ist, wobei ein Schlüssel für eine vorgegebene Zeit Gültigkeit besitzt, d.h. der Nutzer überprüft mittels seines Rundfunkempfängers, ob die Zeit schon erreicht wurde, ab welcher der Schlüssel seine Gültigkeit verliert. Dafür weist der Rundfunkempfänger einen Chronometer auf. Ist der Schlüssel noch gültig, werden erneut in Verfahrensschritt 4 verschlüsselte Daten empfangen. Ist der Schlüssel nicht mehr gültig, wird in Verfahrensschritt 8 überprüft, ob der Nutzer noch Interesse an diesem Datendienst hat. Dies äußert der Nutzer durch Eingaben an seinem Rundfunkempfänger. Ist das der Fall, wird in Verfahrensschritt 2 erneut über das Duplex-Übertragungsverfahren der Datendienstanbieter angewählt, um einen neuen Schlüssel zu erhalten, wobei der Rundfunkempfänger die angeschlossene Sende-/Empfangsstation aktiviert, mit der der Datendienstanbieter angewählt wird. Hat der Nutzer kein Interesse mehr, diesen Datendienst zu nutzen, wird in Verfahrensschritt 9 das Verfahren beendet.

[0032] Als Duplex-Übertragungsverfahren wird hier das GSM-Übertragungsverfahren verwendet und als Rundfunkübertragungsverfahren DAB. Dazu wird eine GSM-Sende-/Empfangsstation in einen DAB-Empfänger integriert oder angeschlossen. Der DAB-Empfänger erhält dann von der GSM-Sende-/Empfangsstation den Schlüssel, den er zur Entschlüsselung der empfangenen verschlüsselten Daten verwendet. Alternativ kann als Sende-/Empfangsstation ein Modem betrieben werden, das an das Telefonnetz angeschlossen ist, falls der Rundfunkempfänger nicht mobil ist.

[0033] In Figur 2 wird in einer Weiterbildung der Erfindung ein Verfahren zur Übertragung von Datensätzen als Flußdiagramm dargestellt.

[0034] In Verfahrensschritt 20 wird das Verfahren begonnen. In Verfahrensschritt 21 fordert ein Nutzer über ein Duplex-Übertragungssystem einen Datensatz von einem Datendienstanbieter an. Dabei wählt der Nutzer entweder wieder den jeweiligen Datendienstanbieter direkt an, oder der Nutzer wählt aus einer im Rundfunkempfänger abgespeicherten Liste einen Datendienstanbieter an, worauf der Rundfunkempfänger mittels einer angeschlossenen Sende-/Empfangsstation den ausgewählten Datendienstanbieter anwählt, um den Datensatz zu laden.

[0035] In Verfahrensschritt 22 erhält der Nutzer mittels des Duplex-Übertragungsverfahrens den angeforderten Datensatz von dem Datendienstanbieter, wobei der Datensatz mittels der Sende-/Empfangsstation empfangen wird und dann an den angeschlossenen Rundfunkempfänger übertragen wird.

[0036] In Verfahrensschritt 23 benutzt der Nutzer

den empfangenen Datensatz, um die Daten mit Mitteln zur akustischen und/oder optischen Darstellung, die der Rundfunkempfänger aufweist, darzustellen. Damit wird z.B. ein Navigationssystem initialisiert, wobei neben den Entfernungsdaten nun auch aktuelle Verkehrsdaten hinzugenommen werden, um einen optimalen Weg zu einem Ziel zu bestimmen.

[0037] In Verfahrensschritt 24 empfängt der Nutzer mittels seines Rundfunkempfängers verschlüsselte Zusatzdaten, mit denen der Nutzer in Verfahrensschritt 25 seinen Datensatz aktualisiert. Damit verfügt das Navigationssystem immer über die aktuellen Verkehrsdaten. Beispielsweise kann so die Existenz eines Staus erkannt werden, die mit dem ursprünglichen Datensatz nicht erkannt worden wäre. Um den privilegierten Zugang zu diesen Zusatzdaten zu ermöglichen, sind in dem ursprünglichen Datensatz Entschlüsselungsdaten enthalten, mit denen die verschlüsselten Zusatzdaten entschlüsselt werden können.

[0038] In Verfahrensschritt 26 wird festgestellt, ob der Datensatz noch gültig ist, d.h. ein Datensatz, den der Nutzer von dem Datendienstanbieter empfängt, hat nur eine zeitlich vorgegebene Gültigkeit. Dies stellt der Rundfunkempfänger mittels eines Chronometers fest, den der Rundfunkempfänger aufweist. Dadurch erreicht der Datendienstanbieter, daß er seinen Datendienst auf einer Oppertunitätsbasis verkaufen kann, ohne einen festen Kundenkreis aufweisen zu müssen. Das ist eine Methode, die zur Zeit von Telefongeseilschaften (Call-by-Call) und Internetzugangsanbietern (Internet-by-Call) anbieten.

[0039] Der Kunde bezahlt durch die Übertragung des ursprünglichen Datensatzes für die vorgegebene Zeit, wie lange er den Datendienst nutzen kann. Dies geschieht, indem der Datendienstanbieter einen bestimmten Preis für die Übertragung über das Duplex-Übertragungssystem festlegt. Bei einem Duplex-Übertragungsverfahren, wie es ein Mobilfunkübertragungsverfahren ist, geschieht dies durch Festlegung der Telefongebühren. Dadurch ist auch der Preis, den der Kunde für den Datendienst bezahlen muß dem Kunden voll transparent.

[0040] Wird im Verfahrensschritt 26 nun festgestellt, daß der Datensatz noch gültig ist, dann wird in Verfahrensschritt 24 fortgefahren, erneut Zusatzdaten zu empfangen, um den ursprünglichen Datensatz weiter auf dem aktuellen Stand zu halten. Ist der Datensatz nicht mehr gültig, wird in Verfahrensschritt 27 überprüft, ob der Nutzer einen neuen Datensatz vom Datendienstanbieter zu laden wünscht, wobei der Nutzer nun auch einen neuen Datendienstanbieter aus wählen kann. Ist dies der Fall, dann wird in Verfahrensschritt 21 vom Nutzer über das Duplex-Übertragungssystem ein neuer Datensatz mittels der Sende-/Empfangsstation angefordert. Hat der Nutzer kein Interesse mehr an diesem Datensatz, dann wird in Verfahrensschritt 28 das Verfahren beendet.

[0041] Auch hier wird wieder das GSM-Mobilfunksystem für das Duplex-Übertragungsverfahren eingesetzt und das DAB-Rundfunkübertragungsverfahren für die Verteilung der Zusatzdaten.

[0042] Besonders geeignet ist dieses Verfahren für Navigationssysteme. Über das Duplex-Übertragungsverfahren wird vom Nutzer ein Datensatz geladen, der aktuelle Verkehrsdaten aufweist. Über ein Rundfunkübertragungsystem werden dann laufend aktualisierte Daten empfangen, um den Datensatz für das Navigationssystem zu erneuern.

[0043] Alternativ sind jedoch weitere Kombinationen möglich, bei denen ein Duplexverfahren mit einem Rundfunkübertragungsverfahren eingesetzt wird. Ist der Kunde an einem Ort, an dem ein Anschluß zu dem verkabelten Telefonnetz vorliegt, kann eine solche Telefonverbindung als Duplex-Übertragungsverfahren verwendet werden, um entweder den Schlüssel zur Entschlüsselung der verschlüsselten Daten zu empfangen oder um den Datensatz zu empfangen.

[0044] Neben den digitalen Rundfunkühertragungsverfahren sind auch analoge Rundfunkübertragungsverfahren zur Übertragung von Daten geeignet, wenn zum Beispiel ein zusätzliches digitales Signal für die Übertragung von Daten mit den analogen Rundfunksignalen übertragen wird. Das bekannte Radio Data System ist ein Beispiel dafür.

Patentansprüche

1. Verfahren zur Übertragung von verschlüsselten Daten, wobei die verschlüsselten Daten mittels eines Rundfunkübertragungsverfahrens zu Nutzern übertragen werden (4), dadurch gekennzeichnet, daß Entschlüsselungsdaten mittels eines Duplex-Übertragungsverfahrens, insbesondere eine Mobilfunk- oder Telefonverbindung, von einem Nutzer durch Anwahl eines Datendienstaabieters angefordert werden (2), daß die Entschlüsselungsdaten vom Datendienstaabieter zu dem Nutzer mittels des Duplex-Übertragungsverfahrens übertragen werden (3) und daß mit den Entschlüsselungsdaten die vom Nutzer mittels des Rundfunkübertragungsverfahrens empfangenen verschlüsselten Daten entschlüsselt werden (5).

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Entschlüsselungsdaten für eine vorgegebene Zeit zur Entschlüsselung der verschlüsselten Daten benutzt werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß dem jeweiligen Nutzer Übertragungszeit für die Übertragung der Entschlüsselungsdaten bei dem Duplex-Übertragungsverfahren in Rechnung gestellt wird, so daß damit die Bereitstellung der verschlüsselten Daten und der Entschlüsselungdaten bezahlt wird.

4. Verfahren nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, daß Datensätze mittels des Duplex-Übertragungsverfahrens zu einem jeweiligen Nutzer übertragen werden (22), daß aktuelle, verschlüsselte Zusatzdaten mittels des Rundfunkübertragungsverfahrens zu den Nutzern übertragen werden (25), daß die verschlüsselten Zusatzdaten mittels Entschlüsselungsdaten, die die Datensätze aufweisen, entschlüsselt werden und daß die entschlüsselten Zusatzdaten zusammen mit den Datensätzen von dem Nutzer genutzt werden (25).

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Datensätze vom jeweiligen Nutzer angefordert werden (21).

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß die Datensätze von den Nutzern eine vorgegebene Zeit genutzt werden (26), worauf dann gegebenenfalls ein neuer Datensatz mittels des Duplex-Übertragungsverfahrens vom Nutzer angefordert und empfangen wird.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß die Übertragungszeit für die Übertragung der Datensätze bei dem Duplex-Übertragungsverfahren dem jeweiligen Nutzer in Rechnung gestellt wird, so daß die Datensätze und die Zusatzdaten vom jeweiligen Nutzer bezahlt werden.

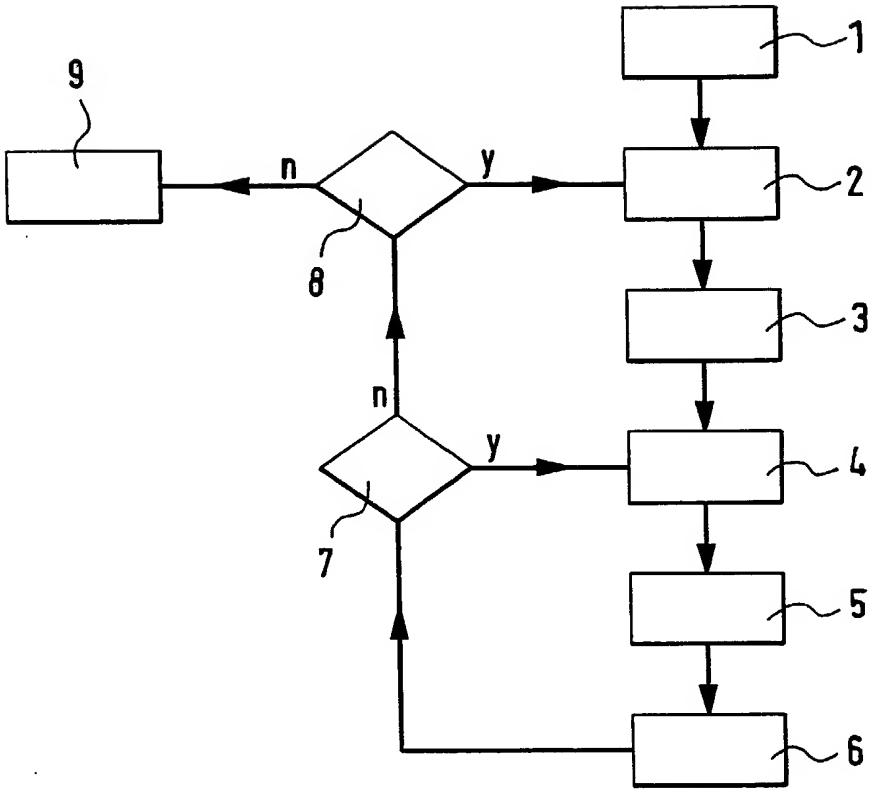

Fig. 1

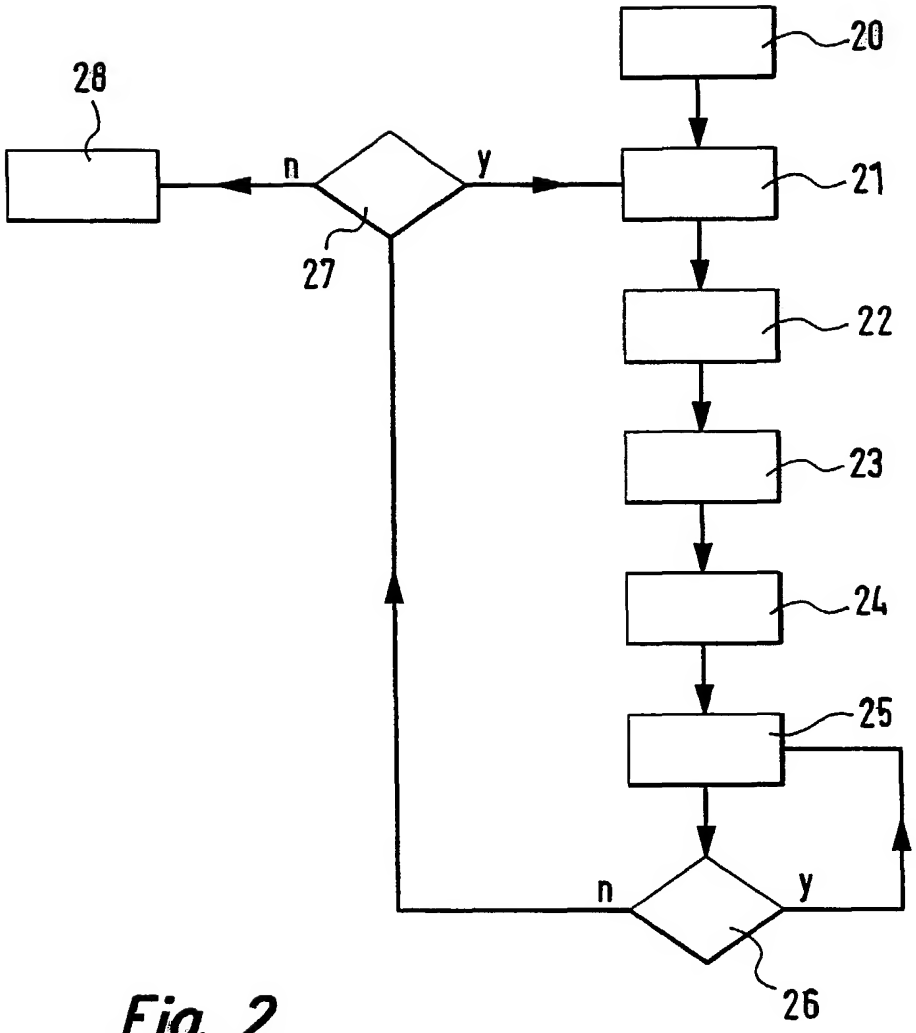

Fig. 2